

Hierarchical Organization of Certification Authorities for Secure Environments



Lourdes López Santidrián
Justo Carracedo Gallardo

Objectives

MAIN OBJECTIVE

To propose a Hierarchical Organization of CAS

Aims:

- General MODEL
- Open MODEL
- Easy solution for Certificate Path Validation

Pilot Experiment

EUIT de Telecomunicación

UNIVERSIDAD DE MADRID

Developments:

- Seckit
- SecServer

SecKit

- Generation of keys (DES, RSA)
- Sending of secure files

SECURE FILE

IDENTIFICATION: Sender Name Sender Certificate

RECEIVER public key:

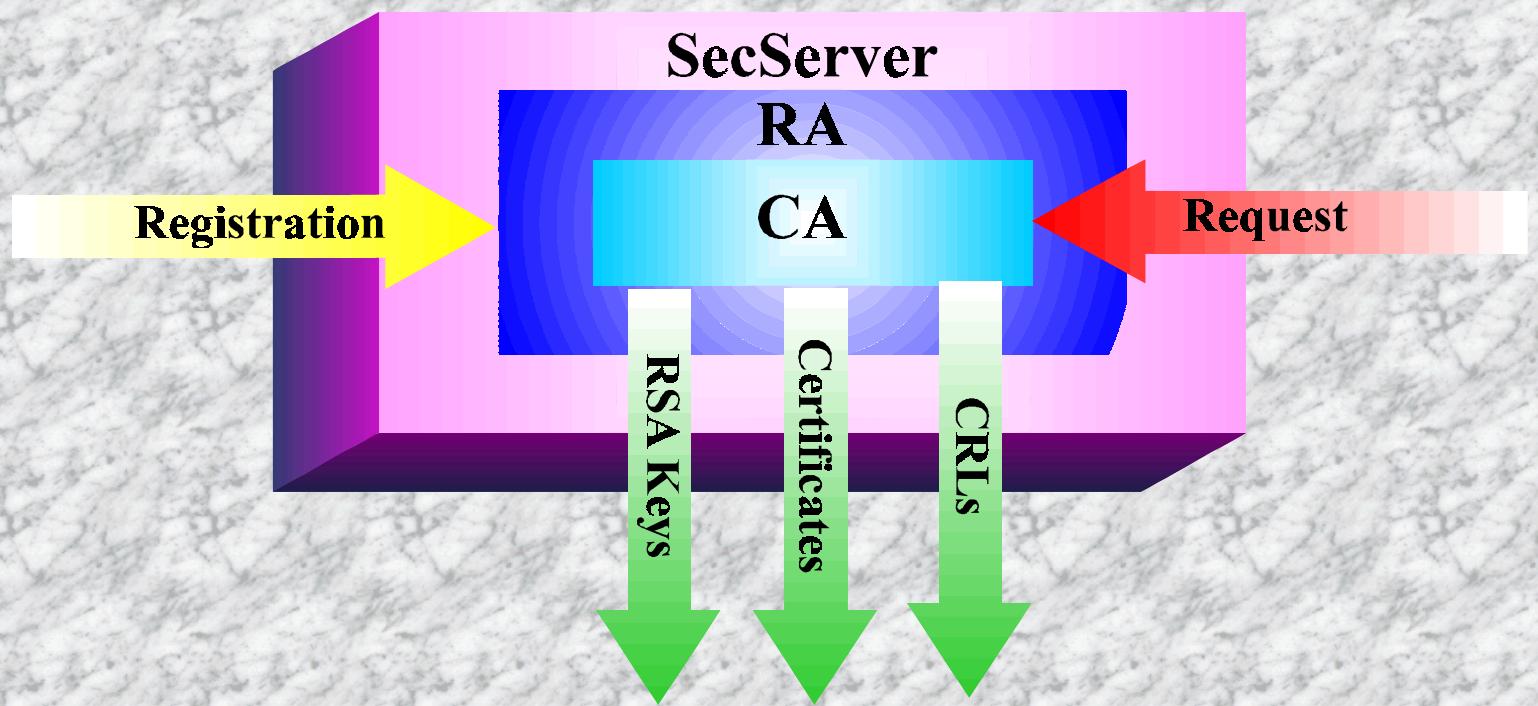
<input type="text"/> Public Key File	<input type="text"/> Certificate	<input checked="" type="text"/> SecServer-request
--------------------------------------	----------------------------------	---

SENDER SECRET KEY: - Insert Smartcard -

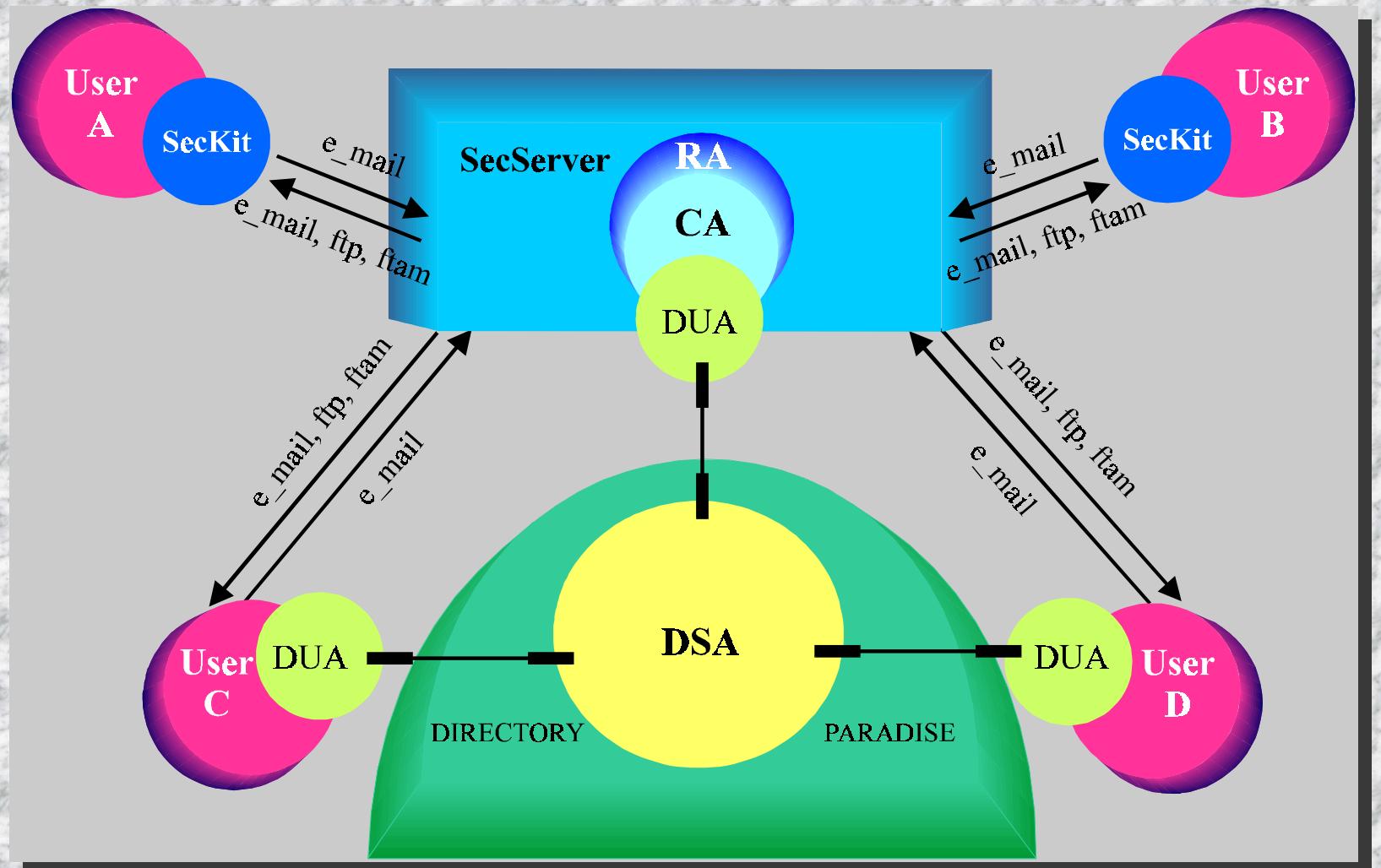
HASH: MD2 MD4 MD5

- Reception of secure files
- Access to the Directory

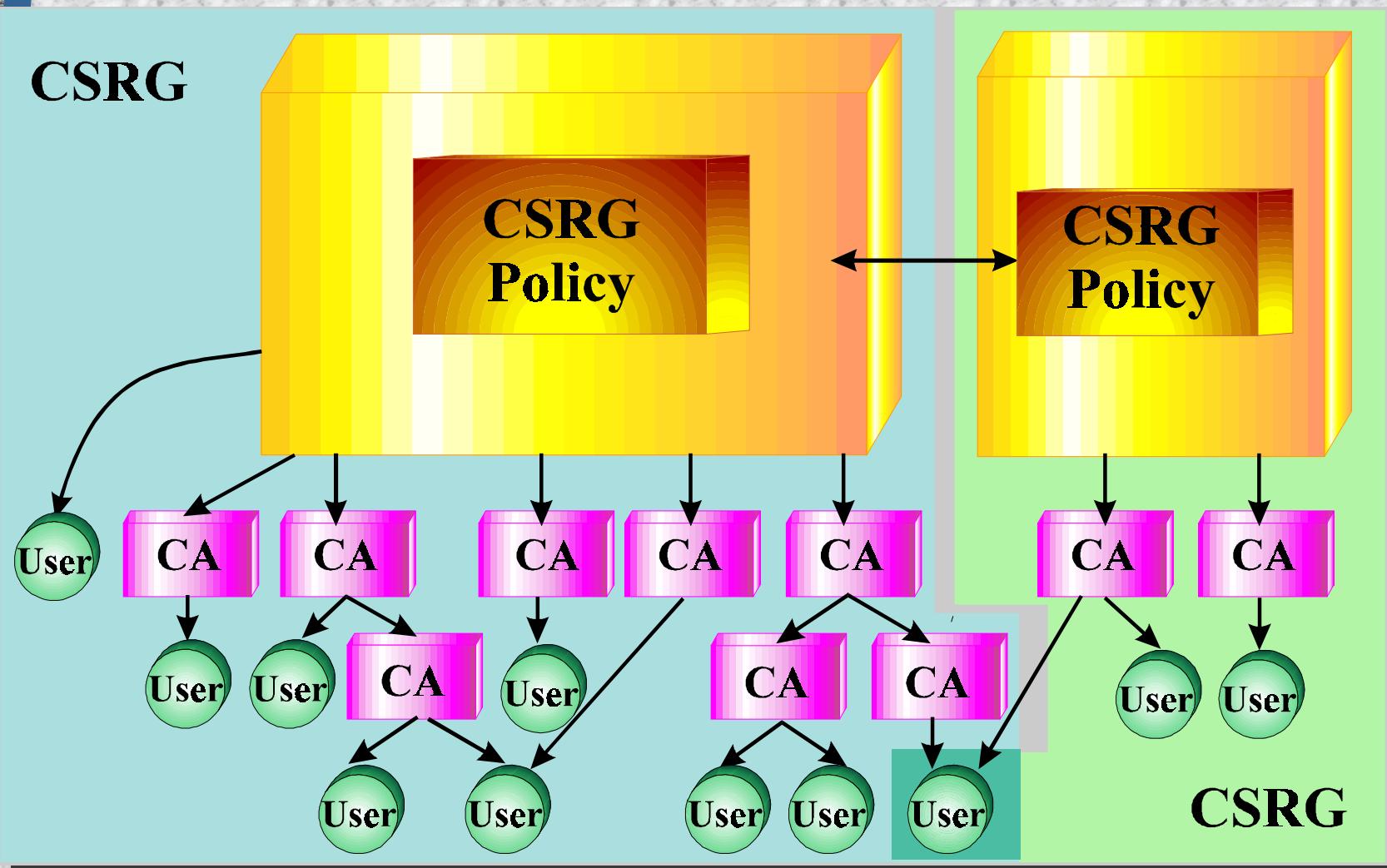
SecServer



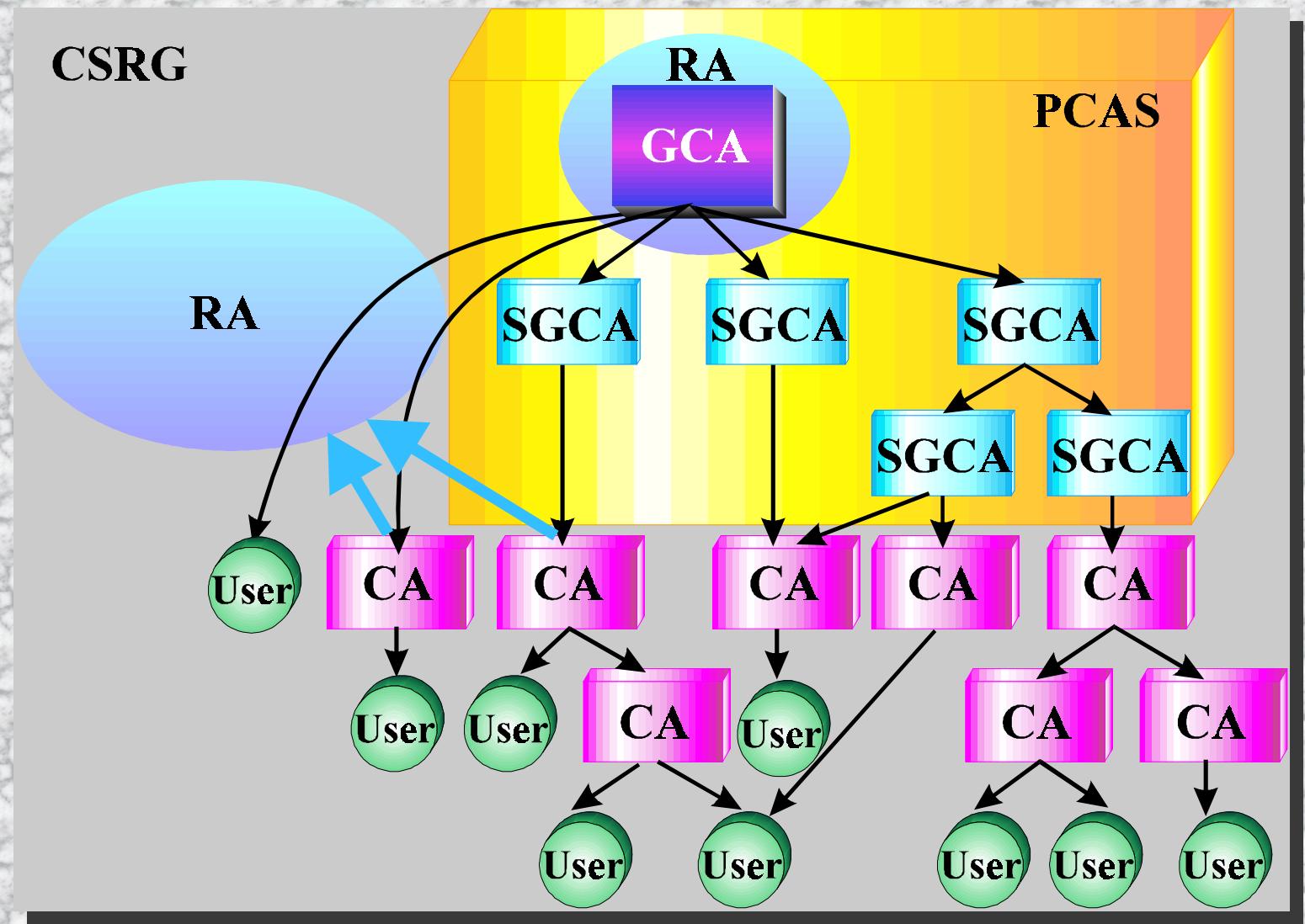
Pilot Environment



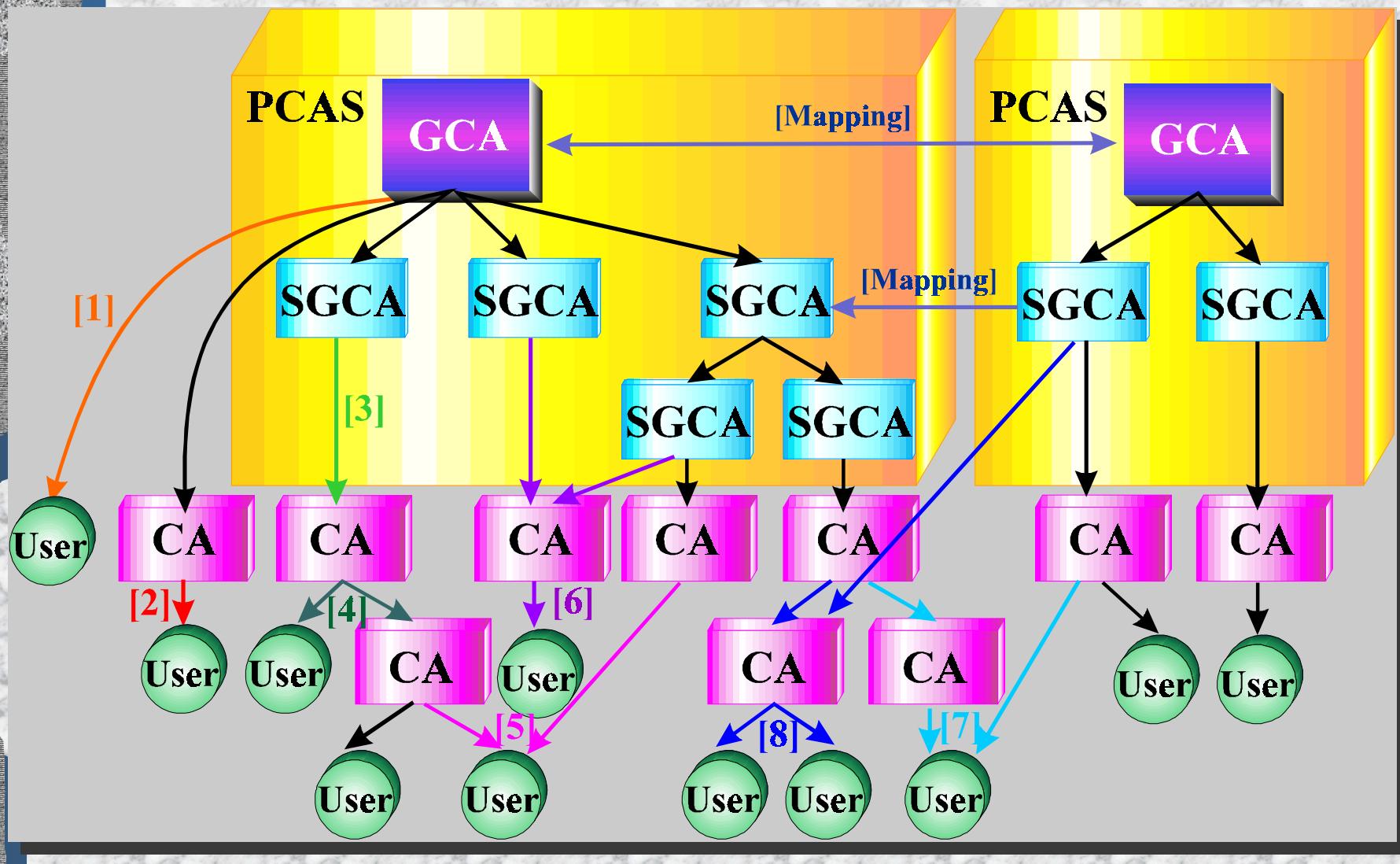
MODEL [1]



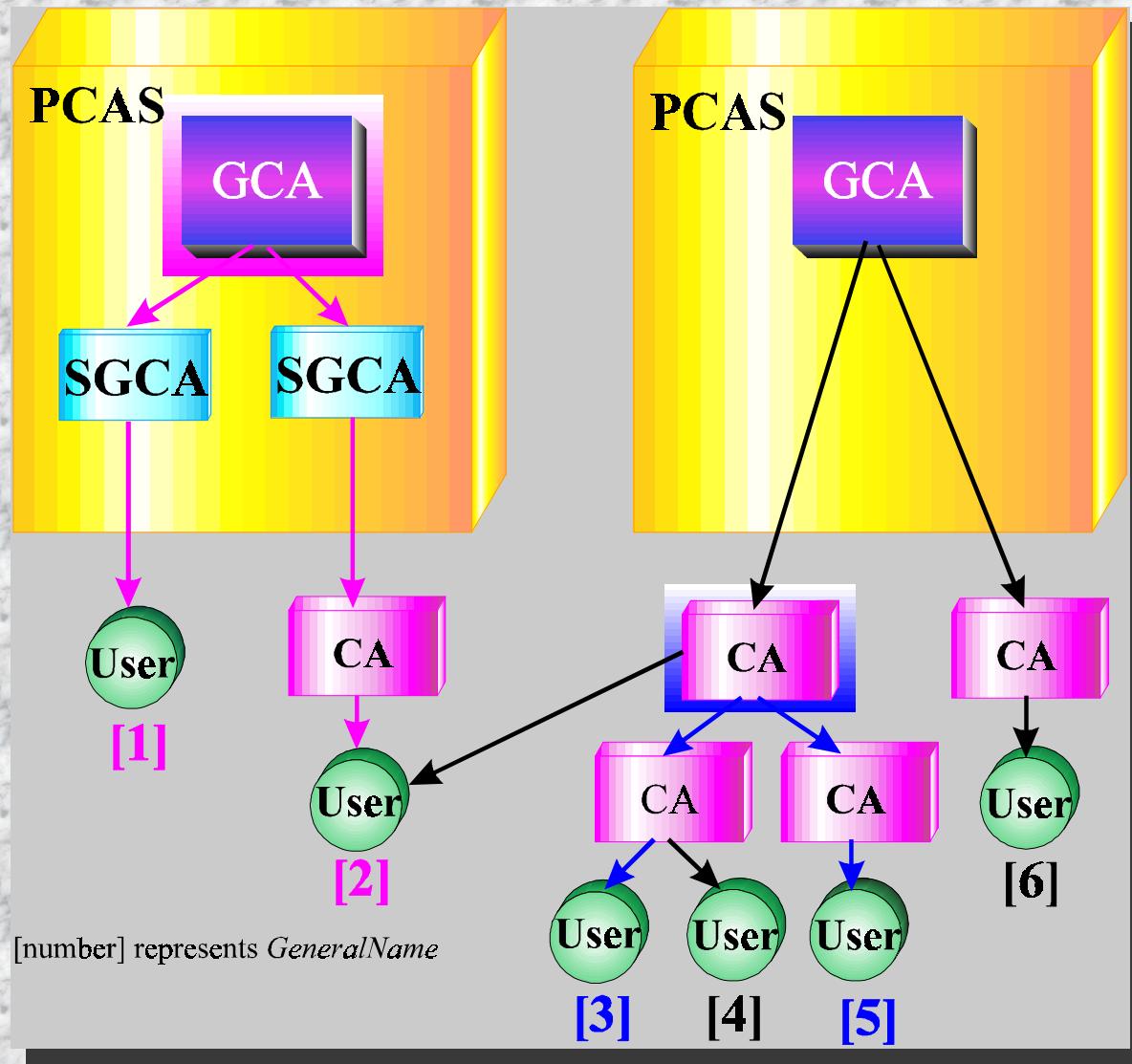
MODEL [2]



MODEL [3]



Certificate Path Validation [1]

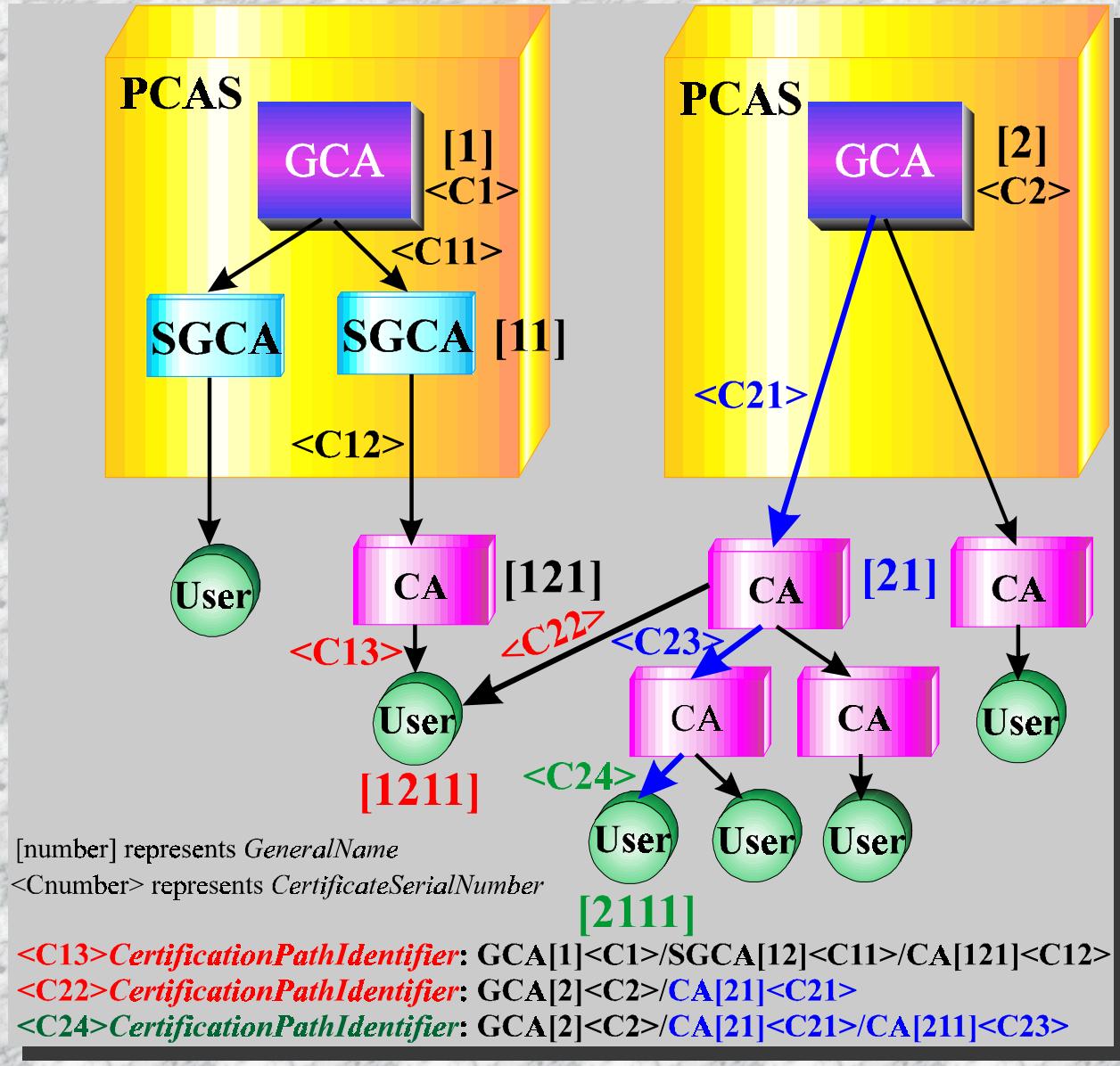


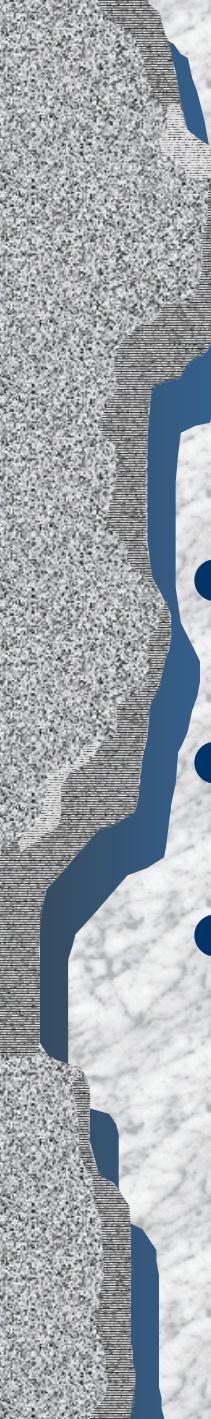
Certificate Path Validation [2]

```
CertificationPathIdentifier ::= SEQUENCE OF  
NewAuthorityKeyIdentifier  
NewAuthorityKeyIdentifier ::= SEQUENCE {  
    autyType                  [0] CertificateType,  
    autyKeyIdentifier         [1] KeyIdentifier OPTIONAL,  
    autyCertIssuer            [2] GeneralNames,  
    autyCertSerialNumber      [3] CertificateSerialNumber }  
CertificateType ::= BIT STRING {  
    groupAuthority           (0),  
    subgroupAuthority         (1),  
    certificationAuthority   (2),  
    user                      (3) }
```

```
NewSubjectKeyIdentifier ::= SEQUENCE {  
    subjectType              [0] CertificateType,  
    subjectKeyIdent          [1] KeyIdentifier OPTIONAL }
```

Certificate Path Validation [3]





Conclusions and Future Work

- Certificate v3 important step ahead
- Go to a general model
- Formal specification of the policy statements